



# Kancelaria Prezesa Rady Ministrów

---

Sekretarz Stanu  
Pełnomocnik Rządu do Spraw Bezpieczeństwa  
Przestrzeni Informacyjnej Rzeczypospolitej Polskiej  
Stanisław Żaryn

DBN.WAKS.416.1.2023  
Warszawa, /data zgodna z podpisem elektronicznym/

**Pan**  
**dr hab. Marcin Wiącek**  
**Rzecznik Praw Obywatelskich**

Szanowny Panie Rzeczniku,

odpowiadając na pismo nr VII.564.25.2022.KSZ, należy na wstępie podkreślić, że z uwagi na obecne uwarunkowania geopolityczne oraz ciągle postępujący rozwój technologiczny w polskiej przestrzeni informacyjnej pojawia się coraz więcej zagrożeń nie tylko dla poszczególnych użytkowników, ale i bezpieczeństwa narodowego RP. Cyberprzestrzeń jest coraz powszechniej wykorzystywana do działań przestępczych – typowo kryminalnych, ale też terrorystycznych, hybrydowych czy wywiadowczych.

Od początku pełnoskalowej agresji Federacji Rosyjskiej na Ukrainę w lutym 2022 r. Polska jest stałym celem wrogich operacji psychologiczno-informacyjnych. Co istotne, dezinformacja stanowi element rosyjskiej doktryny wojennej i jest stosowana przez aparat służb specjalnych jako broń hybrydowa przeciwko społeczeństwom i państwom Zachodu.

W dobie nasilonej walki informacyjnej nowoczesne i kompetentne służby specjalne muszą posiadać narzędzia adekwatne do skali zagrożeń, tak by organy państwa były zdolne do neutralizacji zjawisk niebezpiecznych z punktu widzenia bezpieczeństwa państwa – także w przestrzeni informacyjnej.

Na mocy obowiązujących przepisów prawa właściwe służby zostały wyposażone w uprawnienia umożliwiające im wykonywanie ustawowych zadań wskazanych w art. 5 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. W zakresie blokowania dostępu do treści niebezpiecznych z punktu widzenia bezpieczeństwa państwa stosowany jest art. 180 ustawy Prawo Telekomunikacyjne oraz art. 32 c ustawy o ABW i AW.

Art. 180 ust. 1 ustawy Prawo telekomunikacyjne nakłada na przedsiębiorcę telekomunikacyjnego obowiązek niezwłocznego blokowania połączeń telekomunikacyjnych lub przekazów informacji na żądanie uprawnionych podmiotów, jeżeli połączenia te mogą zagrażać obronności, bezpieczeństwu państwa oraz bezpieczeństwu i porządkowi publicznemu.

Z kolei art. 32 c ustawy o ABW oraz AW reguluje tryb procedury blokady dostępności w systemie teleinformatycznym określonych danych informatycznych lub usług teleinformatycznych mających związek ze zdarzeniem o charakterze terrorystycznym. Ma to szczególne znaczenie w kontekście przeciwdziałania działalności organizacji terrorystycznych, które wykorzystują Internet do propagowania swoich ideologii.

Pragnę zapewnić, że służby na bieżąco realizują swoje ustawowe zadania. Wszelkie działania służb prowadzone są wyłącznie na podstawie i w granicach obowiązujących przepisów prawa.

Z wyrazami szacunku

**Stanisław Żaryn**

/dokument podpisany elektronicznie/